ISSN:2348-2079

Volume-6 Issue-2

International Journal of Intellectual Advancements and Research in Engineering Computations

Authentication System using Master Finger Print

[1] Ashok Prabhu M, [2] Aswin M, [3] Devisri C S, [4] Janani S.R

[1, 2, 3] *UG- Student, Department of CSE, SNS College of Technology, Coimbatore*

[4] *Assistant Professor, Department of CSE, SNS College of Technology, Coimbatore*

[1]*ashokprabhu182@gmail.com*,[2]*devisrii.sudhakar@gmail.com*,[4]*jananiselvaraj.mit@gmail.com*

***Abstract*— In the government forensic department, the need to crack the authentication system of the electronic gadgets or personal devices of criminals and victims has been tremendously increased in the recent years as biometrics plays a major role of authentication. A number of consumer electronic devices, such as smartphones, are beginning to incorporate fingerprint sensors for user authentication. The MasterPrint is a technique where there is a possibility of generating a synthetic or real partial fingerprint that matches one or more template that is stored in the database for a significant number of users Thereby this methodology used by the government and forensic sector to break through the authentication of the device to retrieve the crucial data stored and to access the system. This methodology implied is used to more efficiently to launch indirect attack against fingerprint based authentication system. The algorithm thus used results in increase of efficient MasterPrints with maximum matching rate in comparison to the outcome of the present techniques**.

I. INTRODUCTION

HE major role of the forensics department in the Tgovernment sector is to make use of the methods applied in the acquisition of digital evidence from computer systems and mobile devices for analysis of information involved in criminal investigations of which mobile forensics play a vital role. The job of the forensic experts is to identify criminals and analyze evidence against them. The biggest challenge for the forensics experts is to break the authentication system of the electronic gadgets and devices of the criminals and victims for investigation and evidence.

The need for analysis of digital evidence becomes a crucial element at many crime scenes and this has laid the importance of development of techniques to crack the authentication system like fingerprint based authentication system such as smartphones in order to gain access to personal devices of the crime victims. Cybercrimes and white collar crimes are particularly lucrative because they are generally non-violent crimes, yield high profits and this involves the usage of smartphones and other gadgets to store the confidential data with the help of authentication schemes often with fingerprint based authentication system by the criminals.

Fingerprints are one of the oldest and most widely employed biometric trait used by forensics and law enforcement agencies worldwide. In recent times, there has been a remarkable growth in the utilization of fingerprints for biometric verification in various applications. The purpose of a computer forensic examination to recover data from computers seized as evidence in criminal investigations which in turn has increased the need for efficient means of cracking through the fingerprint based authentication system.

In today's digital age and rise in computer crime, it is no surprise why there is a need to employ forensic analysts for the analysis and interpretation of digital evidence (e.g., computer systems, storage media and devices). The implementation and rapid growth of new technologies has created a few problems to forensic analysts who are now facing the tasks to look after the information not only on the personal computers and laptops but also on tablets and smartphones.

Mobile device forensics is one of the methodology of recovering digital evidence from a mobile device. The operating systems, encryption technologies and protection tools developed by smartphone companies like Nokia, Samsung, LG, Huawei, Apple and more obliges analysts to keep up with latest developments at a faster rate than ever before. Today's new advanced devices are produced at higher rates and extracting information from them, even though these device are highly protected.

There are many techniques that analyze and gather forensic data from mobile devices, from the less intrusive manual extraction to the invasive. But the challenge in today scenario is to break the advanced authentication system to access such devices. Thus it is necessary to develop techniques for effective means of cracking the electronic gadgets.

Computer forensics is the new frontier of criminal investigation and it is growing daily. As technology enhances the crimes associated by using technology in criminal activity is also increasing rapidly. Computers can yield evidence of a wide range of criminal and other

unlawful activities; criminals engaged in network-based crimes are not the only ones who store information on smartphones and other devices. Many criminals engaged in murder, kidnapping, sexual assault, extortion, drug dealing, auto theft, espionage and terrorism, gun dealing, robbery/burglary, gambling, economic crimes, confidence games, and criminal hacking (e.g., Web defacements and theft of computer files) maintain files with incriminating evidence on their computer with some high security. Sometimes the information on the computer is the key to identifying a suspect and sometimes the computer yields the most damning evidence. Thus, the breaking of the authentication systems using MasterPrint comes into play.

The solution to this problem is to identify the MasterPrint that match with a large number of fingerprints that is stored in the database which is originating from different users and possibly to generate MasterPrints synthetically.

For a MasterPrint, we need to create a synthetic fingerprint that fools a fingerprint verification system. The verification system not only has to recognize that the image is a fingerprint, but also matches the fingerprint to many different identities. Therefore, a generator network need to combine with a way of searching fingerprints that are suitable for MasterPrints.

The generation of the MasterPrints involves the process of reading the fingerprint and analyzing the dataset for matching prints that has a high matching rate which are considered as the Sampled MasterPrints from which the Synthetic MasterPrints are generated by manipulation to increase the Imposter match rate. The result reveals that even if a MasterPrint matches with a small number of partial fingerprints which is stored in the data set. The percentage of subjects that it matches against is quite high. Thus the implementation of the proposed technique increases the false match rate of the MasterPrint than the existing methodology.

II. PRIOR WORK

The security of biometric systems has been extensively studied in the past two decades. It is well known that in spite of its numerous advantages, a fingerprint-based biometric system is potentially vulnerable to a variety of attacks. The attack only needs a fake biometric without any knowledge of the matcher, image specifications or database access privileges, its vulnerability is higher compared to the other attacks. A spoof attack can be launched by (a) lifting the residual fingerprint of a user from the phone or any other surface, (b) creating a dummy finger from the lifted impression; and (c) placing the dummy finger on the fingerprint sensor. Another type of attack involves the reconstruction of a fingerprint image from a minutiae template.

A. Brute force attack

A crude brute force attack with a large number of input fingerprints can be used. Ratha et al. [10] established the relationship between the number of brute force attack attempts and the number of minutiae that is expected to match. They showed that the search space for guessing the fingerprint to be matched can be prohibitively large. However, for a mobile device, where only a portion of the full fingerprint is used, this search space would be much smaller.

B. Dictionary based guessing attack

In contrast to a brute force attack, a dictionary attack tries only those possibilities which lead to success. For example, if an attacker tries to access a password protected system by trying the 10 most common passwords in that database and using a listing of known accounts, he could be expected to succeed and it depends on the dataset and dictionary size.

Existing work has only modeled the observed minutiae feature distribution statistically to compute the Probability of Random Correspondence, which is actually the false match rate, for a full fingerprint dataset. The matchers does not utilize both minutiae, texture information and designing more effective fusion schemes to combine the information presented by multiple partial impressions of a user.

III. MASTERPRINT

The generation of MasterPrint is based on two approaches: Sampled (one where the print is selected from an existing dataset of real fingerprints) and Synthetic (the print is generated synthetically). For the first approach, a fixed dataset is used as the training set from which the MasterPrint is sampled. These MasterPrints selected directly from a dataset are known as Sampled MasterPrint or SAMP. The synthetically created MasterPrints with the help of the SAMP are termed as Synthetic MasterPrint or SYMP.

The fingerprint can be obtained for both full fingerprint and partial fingerprint authentication systems. But of which it is highly effective to generate synthetic fingerprints for partial fingerprint authentication systems. Thus it is necessary to generate the partial fingerprints from the full fingerprints of the users. This creates partial fingerprints of a particular size by cropping the full prints using an overlapping window that moved from top-to-bottom and left to right with a 50% overlap between adjacent windows.

Fig. 1. Minutiae Extraction

The next stage of processing involves minutiae extraction that makes use of the commercial fingerprint verification software Verifinger 6.1 SDK to identify the matching fingerprints. The matching fingerprints are obtained depending upon the False Match Rate and True Match Rate values.

Generating MasterPrints by sampling a fingerprint dataset (training set) is rather straightforward. The "Imposter Match Rate" (IMR) - which is the number of false matches when a fingerprint is compared against images of other fingers (impostors) - is computed for all candidate prints. The prints with maximum IMRs are selected from the dataset. However, since these SAMP are identified from an existing dataset. Moreover, it may not be always possible to find a MasterPrint in a selected dataset. To improve the IMR of MasterPrint, we also have the possibility of creating a synthetic MasterPrint by altering a SAMP. The final step of the proposed objective is to generate improved MasterPrints synthetically by maximizing their IMR over a training dataset. It results in highly effective synthetic impressions that are falsely accepted by the matcher. The SAMP found from the training dataset are used as the initial seed in the synthetic MasterPrint generation process.

IV. RESULTS

To investigate whether the generated MasterPrints successfully match with a large number of fingerprint impressions pertaining to multiple subjects, the maximum value of the MasterPrint is to be determined. An authentication system would permit a user to offer their fingerprints multiple times in the case of a failed authentication attempt. But in the latter case, multiple MasterPrints are identified, and a successful authentication is done when an incorrect subject matches with the target subject.

The data is to be collected using Authentec AES3400 sensor. The fingerprints from this dataset were used without any modifications, as these fingerprints were already partial in nature. It is assumed that there are substantial differences among the partial fingerprints captured from the same finger. From the optical dataset, partial fingerprints of size 150 × 150 pixels are created. To create the training and test datasets, each dataset is divided into two disjoint sets each containing data corresponding to 50% of the fingers.

This partitioning of each dataset into finger-disjoint training and test sets is done 5 times, resulting in 5 different estimates for dictionary attack success. The experiments are performed in two phases: " imagelevel comparison" phase, where best SAMPs are identified by an "all-to-all" matching and " finger-level comparison " phase, where the selected SAMPs and the SYMPs generated from them are used to attack the subjects in the test set.

At first, the IMRs of all the partial fingerprints in the training dataset are computed and the print with the highest IMR is selected. The variation in the combined average finger-level IMR is increased when increasing the number of impressions per finger. For example, at an FMR of 0.1%, the IMR increased from 1.32% to 23.9% using independent SAMPs. Further, it can be observed that the sequential SAMPs performed better than the independent SAMP irrespective of the number of impressions per finger. The IMR using sequential SAMP at FMR is 0.1% increased from 2.4% to 26.5%.

V. CONCLUSION

The generation of the Synthetic MasterPrint using the hill climbing methodology provides a more effective way of generating the prints that match with a large population of fingerprint samples than that provided by the existing technique with a increase in the outcome comparatively. Thus it provides an improved way of generating MasterPrint with more efficiency that can be used in the government and forensics department to yield a better result.

REFERENCES

[1] Aditi Roy, "MasterPrint: Exploring the Vulnerability of Partial Fingerprint-basedAuthentication Systems" IEEE Transactions onInformation Forensics and Security, 2017

[2] K. Cao, E. Liu, L. Pang, J. Liang, and J. Tian "Fingerprint matching by incorporating minutiae discriminability" in International Joint Conference on Biometrics (IJCB), 2011

[3] Cao and Jain Cao, K., and Jain, A. K. "Learning fingerprint reconstruction: From minutiae to image" IEEE Transactions on information forensics and security, 2015

[4] B. B. Han, C. A. Marciniak, and W. C.Westerman "Fingerprint sensing and enrollment" US Patent App. 14/244,143, Apr 3 2013

[5] K. Jain, Y. Chen, and M. Demirkus, "Pores and ridges: High-resolution fingerprint matching using level 3 features" IEEE Transactions on Pattern Analysis and Machine Intelligence, 29(1):15–27, January 2007

[6] E. Marasco and A. Ross, "A survey on antispoofing schemes for fingerprint recognition systems" ACM Computing Surveys (CSUR), 47(2):28, 2015

[7] T. Matsumoto, H. Matsumoto, K. Yamada, and S. Hoshino., "Impact of artificial gummy fingers on fingerprint systems" International Society for Optics and Photonics, 2002

[8] Nagar, H. Choi, and A. K. Jain "Evidential value of automated latent fingerprint comparison: an empirical approach" IEEE Transactions on Information Forensics and Security, 7(6):1752–1765, 2012

[9] Philip Bontrager, Togelius, NasirMemon"DeepMasterPrint: Generating Fingerprints for Presentation Attacks" IET Biometrics,2017

[10] Ratha, Connell, and BolleRatha, N. K.; Connell, J. H.; and Bolle, R. M. 2001.An analysis of minutiae matching strength in Audio-and VideoBased Biometric Person" 2001

[11] Ross. Information Fusion in Fingerprint Authentication.PhD thesis, Michigan State University, 2003.

[12] Sousedik, C., and Busch, C, "Presentation attack detection methods for fingerprint recognition systems: a survey" IET Biometrics,2014